v7.n8.2026

REVISTA CIENTÍFICA - RECIMA21 ISSN 2675-6218

TECNOLOGIA *BLOCKCHAIN* NA CADEIA DE CUSTÓDIA DE VESTÍGIOS: GARANTIA DA INTEGRIDADE PROBATÓRIA NO PROCESSO PENAL BRASILEIRO

BLOCKCHAIN TECHNOLOGY IN THE CHAIN OF CUSTODY OF CRIMINAL EVIDENCE: ENSURING EVIDENTIARY INTEGRITY IN BRAZILIAN CRIMINAL PROCEDURE

TECNOLOGÍA BLOCKCHAIN EN LA CADENA DE CUSTODIA DE VESTIGIOS: GARANTÍA DE LA INTEGRIDAD PROBATORIA EN EL PROCESO PENAL BRASILEÑO

Fabrício Bittencourt da Cruz[1], Murilo Inoue Michaloski[2], Bruno Vieira Henneberg[3]

e788681
https://doi.org/10.47820/recima21.v7i8.8681

PUBLICADO: 08/2026

RESUMO

Este estudo investiga se a implementação da tecnologia *blockchain* nas etapas de fixação, recebimento e processamento da cadeia de custódia é suficiente para garantir a autenticidade e a integridade probatórias diante do risco de adulteração no contexto do processo penal brasileiro. A hipótese sustenta que a introdução dessa tecnologia é adequada para assegurar a autenticidade e a integridade das provas, proporcionando segurança jurídica superior à dos métodos convencionais de documentação. Metodologicamente, adota-se abordagem qualitativa e o método hipotético-dedutivo, configurando pesquisa exploratória e explicativa realizada por meio de revisão bibliográfica e documental indireta. O referencial teórico baseia-se em artigos científicos sobre *blockchain* e obras jurídicas sobre cadeia de custódia e as consequências processuais de sua quebra. Os resultados indicam que a *blockchain* é um mecanismo potencialmente relevante, porém não suficiente. Isto porque assegura a integridade das etapas de fixação, recebimento e processamento a partir do registro, mas não alcança as falhas de autenticidade anteriores à inserção dos dados e depende tanto de uma arquitetura híbrida compatível com a lei de proteção de dados pessoais, quanto de regulamentação nacional uniforme.

PALAVRAS-CHAVE: Cadeia de custódia. Processo penal brasileiro. *Blockchain*. Autenticidade probatória. Integridade probatória.

ABSTRACT

This study investigates whether the implementation of blockchain technology in the recording, receipt, and processing stages of the chain of custody is sufficient to ensure evidentiary authenticity and integrity in view of the risk of tampering in the context of Brazilian criminal proceedings. The hypothesis is that the introduction of this technology is adequate to ensure the authenticity and integrity of evidence, providing greater legal certainty than conventional documentation methods. Methodologically, the study adopts a qualitative approach and the hypothetical-deductive method, constituting exploratory and explanatory research conducted through an indirect bibliographic and documentary review. The theoretical framework is based on scientific articles on blockchain and legal scholarship concerning the chain of custody and the procedural consequences of its breach. The findings indicate that blockchain is a potentially relevant, but insufficient, mechanism.

[1] Doutor em Direito pela Universidade de São Paulo (USP). Professor Associado na Universidade Estadual de Ponta Grossa (UEPG).
[2] Graduando em Direito na UEPG. Bolsista IC Fundação Araucária - NAPI Segurança Pública e Ciências Forenses.
[3] Graduando em Direito pela UEPG. Bolsista IC Fundação Araucária - NAPI Segurança Pública e Ciências Forenses.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

This is because it ensures the integrity of the recording, receipt, and processing stages from the moment the information is registered, but it cannot address authenticity failures that occur before data entry and depends both on a hybrid architecture compatible with personal data protection law and on uniform nationwide regulation.

KEYWORDS: *Chain of custody. Brazilian criminal procedure. Blockchain. Evidentiary authenticity. Evidentiary integrity.*

RESUMEN

Este estudio investiga si la implementación de la tecnología blockchain en las etapas de fijación, recepción y procesamiento de la cadena de custodia es suficiente para garantizar la autenticidad y la integridad probatorias ante el riesgo de adulteración en el contexto del proceso penal brasileño. La hipótesis sostiene que la introducción de esta tecnología es adecuada para asegurar la autenticidad y la integridad de las pruebas, proporcionando una seguridad jurídica superior a la de los métodos convencionales de documentación. Metodológicamente, se adopta un enfoque cualitativo y el método hipotético-deductivo, configurándose una investigación exploratoria y explicativa realizada mediante una revisión bibliográfica y documental indirecta. El marco teórico se basa en artículos científicos sobre blockchain y en obras jurídicas sobre la cadena de custodia y las consecuencias procesales de su ruptura. Los resultados indican que la blockchain es un mecanismo potencialmente relevante, aunque insuficiente. Esto se debe a que garantiza la integridad de las etapas de fijación, recepción y procesamiento desde el momento del registro, pero no alcanza las fallas de autenticidad anteriores a la incorporación de los datos y depende tanto de una arquitectura híbrida compatible con la legislación de protección de datos personales como de una regulación nacional uniforme.

PALABRAS CLAVE: *Cadena de custodia. Proceso penal brasileño. Blockchain. Autenticidad probatoria. Integridad probatoria.*

INTRODUÇÃO

A discussão sobre a autenticidade das provas no processo penal acompanha a própria história do direito punitivo. Já em 1764, Beccaria (2015, p. 15) advertia que, quando os indícios do delito não se sustentam senão uns pelos outros e a força de várias provas depende da verdade de uma só, a destruição da única prova que parecia certa derruba todas as demais.

Na atualidade brasileira, mesmo após o advento da Lei 13.964/2019, que regulamentou a cadeia de custódia nos artigos 158-A a 158-F do Código de Processo Penal brasileiro (CPP), persistem questionamentos sobre a confiabilidade de provas periciais, especialmente em âmbito digital, a partir do que se passou a denominar quebra da cadeia de custódia.

A tecnologia *blockchain* mostra-se relevante diante dessa problemática por sua capacidade de assegurar registros auditáveis e rastreáveis nas etapas de fixação, recebimento e processamento de evidências, com potencial para fortalecer a confiança na integridade de tais evidências como prova na justiça criminal.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

A preocupação com a integridade da cadeia de custódia de evidências digitais já motivou diversas iniciativas normativas em âmbito internacional. Na China (2019), o *Blockchain Information Service Management Regulations* versa sobre o desenvolvimento tecnológico seguro da *blockchain*. Na União Europeia (2014), o *eIDAS Regulation* estabelece parâmetros compatíveis com a imutabilidade e a auditabilidade dos registros. Além disso, a Convenção de Budapeste sobre o Cibercrime, promulgada no Brasil pelo Decreto 11.491/2023, reforça a necessidade de implementação de instrumentos tecnológicos adequados a assegurar a integridade da cadeia de custódia penal.

Apesar desse movimento, ainda se observa relevante lacuna na literatura e na prática jurídica brasileiras quanto à aplicação da *blockchain* na cadeia de custódia. O ordenamento brasileiro exige o controle contínuo do vestígio, mas não estabelece parâmetros técnicos ou normativos para o uso de ferramentas tecnológicas para tanto. Há, portanto, um descompasso, já que a norma prescreve procedimento a ser implementado, mas sua aplicação permanece deficiente.

Este trabalho foi desenvolvido a partir do seguinte problema de pesquisa: a implementação de tecnologia *blockchain* na cadeia de custódia de vestígios, particularmente nas etapas de fixação, recebimento e processamento previstas no artigo 158-B do CPP, é suficiente para garantir a autenticidade e a integridade probatórias diante do risco de adulteração de evidências no processo penal?

Como hipótese a orientar este estudo sustenta-se que a introdução da tecnologia *blockchain* nessas fases é adequada para assegurar a autenticidade e a integridade das provas, proporcionando segurança superior à dos métodos convencionais de documentação da cadeia de custódia.

O objetivo geral da pesquisa consiste em analisar a suficiência da tecnologia *blockchain* nas etapas de fixação, recebimento e processamento da cadeia de custódia de vestígios, previstas no art. 158-B do CPP, como instrumento de garantia da autenticidade e da integridade probatórias.

A pesquisa possui dois objetivos específicos: (i) apresentar as vulnerabilidades da cadeia de custódia nas etapas do art. 158-B e descrever as propriedades da *blockchain* aplicáveis à sua superação; e (ii) discutir os desafios para a implementação de *blockchain* na custódia de evidências no sistema de persecução penal brasileiro.

A relevância do tema decorre da digitalização da atividade jurisdicional e investigativa, que levou à utilização de provas integralmente digitais no processo penal brasileiro e esse é o contexto em que se insere a pesquisa. Afinal, conforme o Relatório Justiça em Números 2026,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

os processos judiciais eletrônicos alcançaram 100% no primeiro grau e 99,7% no segundo grau de jurisdição do Poder Judiciário brasileiro (Brasil, 2026).

1. REFERENCIAL TEÓRICO

O estudo articula dois campos teóricos: o instituto processual penal da cadeia de custódia e a tecnologia de registro distribuído *blockchain*.

No primeiro campo, adota-se como ponto de partida a definição legal de cadeia de custódia (art. 158-A do CPP) e a sequência de dez etapas fixada pelo art. 158-B, com destaque para a fixação, o recebimento e o processamento, em razão do peso dessas etapas na verificação da autenticidade do elemento probatório (Brasil, 2019). A leitura do instituto apoia-se nos princípios da mesmidade (Prado, 2021a) e da desconfiança (Menezes; Borri; Soares, 2018).

Quanto às consequências da quebra da cadeia de custódia, o referencial incorpora a divergência entre a corrente que sustenta a ilicitude da prova, com sua inadmissibilidade ou exclusão do processo e a que remete o problema ao plano da valoração probatória, bem como a tese da contaminação das provas derivadas. Esse quadro teórico é confrontado com a jurisprudência do Superior Tribunal de Justiça (STJ) sobre a matéria, especialmente o AgRg no RHC 143.169/RJ (Brasil, 2023c), o HC 653.515/RJ (Brasil, 2021), o RHC 205.441/GO (Brasil, 2025c) e o RHC 218.358/PI (Brasil, 2025d).

No campo tecnológico, parte-se do desenho original da *blockchain* (Nakamoto, 2008) e de sua caracterização como livro-razão digital compartilhado em rede de grupos independentes (Laurence, 2018), com a descrição técnica de blocos, cabeçalho, lista de transações, *timestamp*, *hash* e raiz de Merkle fornecida por Conceição e Rocha (2020). Os limites da tecnologia são examinados a partir de duas balizas: a função *hash* como mecanismo de aferição de integridade do pacote de dados, e não de autenticidade da fonte (Fisberg, 2025); e o Problema do Oráculo, relativo à confiabilidade das informações geradas fora da rede (Egberts, 2017; Al-Breiki et al., 2020; Pasdar; Lee; Dong, 2023).

Completa o referencial o conjunto normativo e institucional que baliza a custódia de evidências digitais: a ABNT NBR ISO/IEC 27037 (ABNT, 2013), a Convenção de Budapeste (Brasil, 2023a), as normativas estrangeiras sobre registros digitais e criptoativos (China, 2019; União Europeia, 2014; 2023; Estados Unidos, 2024; Emirados Árabes Unidos, 2022), os projetos de lei brasileiros em tramitação (PL 4.939/2020 e PL 1.195/2025) e a Portaria 391/2025 do Conselho Nacional de Justiça (CNJ), examinados nas seções 3.1 a 3.4.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

2. METODOLOGIA

A pesquisa adota abordagem qualitativa de natureza teórico-dogmática e o método hipotético-dedutivo, partindo do cotejo entre a hipótese, a literatura especializada em direito processual penal e em *blockchain* e as fontes documentais selecionadas. Quanto aos objetivos, caracteriza-se como exploratória e explicativa.

A pesquisa valeu-se de documentação indireta, consistente em documentos normativos e institucionais nacionais e internacionais. Foram analisados os arts. 158-A a 158-F do CPP, a Portaria SENASP 82/2014, a ABNT NBR ISO/IEC 27037, a Convenção de Budapeste (Decreto 11.491/2023), o *Blockchain Information Service Management Regulations* chinês, o Regulamento eIDAS e o MiCA da União Europeia, o FIT21 dos Estados Unidos da América e a Lei 4/2022 dos Emirados Árabes Unidos, bem como os projetos de lei em tramitação no Brasil (PL 4.939/2020 e PL 1.195/2025), a Portaria 391/2025 do CNJ e decisões do STJ.

Na elaboração deste trabalho, utilizou-se a ferramenta de inteligência artificial Claude (Anthropic) para revisão gramatical e ajustes de estilo.

3. RESULTADOS E DISCUSSÃO

3.1. A cadeia de custódia de evidências criminais

A cadeia de custódia é definida pelo próprio texto legal como o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, com o objetivo de rastrear sua posse e manuseio desde o reconhecimento até o descarte (Brasil, 2019, art. 158-A).

Antes da Lei 13.964/2019, o CPP não regulamentava a cadeia de custódia. O instituto existia apenas no plano administrativo, por força da Portaria SENASP 82/2014, com aplicação restrita à Força Nacional de Segurança Pública (Brasil, 2014). A referida lei, ao inserir os arts. 158-A a 158-F no CPP, conferiu ao instituto status de norma processual penal vinculante para todos os órgãos de persecução criminal do país (Brasil, 2019).

O art. 158-B do CPP enumerou dez etapas: reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte. Cada etapa constitui um elo na cadeia, e a falha em qualquer delas fragiliza a integridade do conjunto probatório (Brasil, 2019, art. 158-B). Três etapas merecem destaque especial neste estudo em razão do peso na verificação da autenticidade do elemento probatório: a fixação, o recebimento e o processamento.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

A fixação consiste na "descrição detalhada do vestígio conforme se encontra no local do crime, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável sua descrição no laudo pericial" (Brasil, 2019, art. 158-B, inc. III). É nessa etapa que se registra o estado original da evidência antes de qualquer manuseio, constituindo o ponto zero da rastreabilidade probatória.

O recebimento é o ato formal de transferência da posse do vestígio ao órgão pericial, devendo ser documentado com o número do procedimento policial, local de origem, nome de quem transportou, código de rastreamento, natureza do exame, tipo do vestígio, protocolo e assinatura do recebedor (Brasil, 2019, art. 158-B, inc. VII).

Trata-se de elo crítico por consistir no momento em que a custódia passa dos agentes de campo aos peritos, e o art. 158-D exige recipientes selados por intermédio de lacres individualizados, com o registro individualizado de cada rompimento (Brasil, 2019, art. 158-D).

O processamento é o exame pericial propriamente dito, abrangendo a manipulação do vestígio de acordo com a metodologia adequada às suas características, cujo resultado deverá ser formalizado em laudo produzido por perito (Brasil, 2019, art. 158-B, inc. VIII).

Contudo, a positivação da cadeia de custódia não eliminou vulnerabilidades que podem ensejar o comprometimento da integridade probatória na prática.

A primeira vulnerabilidade é normativa. A Lei 13.964/2019 fixou as etapas, mas não disciplinou os protocolos técnicos de execução, remetidos na prática a cada órgão pericial e a normas sem força de lei, como a ABNT NBR ISO/IEC 27037, que reúne diretrizes para a identificação, a coleta, a aquisição e a preservação de evidências digitais (ABNT, 2013). A ausência de critérios legais objetivos dificulta aferir, em concreto, a adequação do procedimento adotado, sobretudo no campo das provas digitais (ponto retomado na seção 3.4, ao se demonstrar como a *blockchain* operacionaliza essas diretrizes).

A segunda vulnerabilidade decorre do acesso ao vestígio digital por particular interessado antes da perícia oficial. No AgRg no RHC 143.169/RJ, relacionado a uma operação policial que apurava furtos eletrônicos, a instituição financeira lesada havia acessado os dados digitais antes da realização da perícia policial. Esse fato, aliado à insuficiência documental sobre o acondicionamento dos equipamentos e os procedimentos de extração dos dados, levou o STJ a reconhecer a inadmissibilidade das provas digitais obtidas (Brasil, 2023c).

A terceira vulnerabilidade é o envio do vestígio sem lacre ou acondicionamento adequado. No HC 653.515/RJ, a substância entorpecente havia sido encaminhada à perícia sem observância do art. 158-D do CPP (garantia de inviolabilidade e de idoneidade dos vestígios coletados), e o STJ entendeu que a condenação pelo tráfico não poderia subsistir, pois a

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

irregularidade impedia afastar a possibilidade de substituição ou adulteração do material (Brasil, 2021).

A quarta vulnerabilidade, particularmente acentuada nas provas digitais, reside na dificuldade de perceber alterações ocorridas durante sua custódia. A natureza imaterial desses vestígios amplia os riscos de perda, degradação ou modificação do conteúdo (Fisberg, 2025, p. 4). Também devem ser considerados riscos de alteração decorrentes das condições físicas e técnicas de conservação do material digital, inclusive por fatores ambientais, mecânicos ou temporais (Vieira; Santos, 2025).

Por fim, há uma vulnerabilidade estrutural relacionada à assimetria entre acusação e defesa no acesso ao material probatório. Como os elementos de prova são, em regra, produzidos e mantidos pelos órgãos estatais de persecução, a defesa pode enfrentar limitações relevantes para controlar sua conservação e percurso até os autos do processo judicial (Menezes; Borri; Soares, 2018).

3.2. Autenticidade probatória e consequências da quebra da cadeia de custódia

O elemento de prova cuja autenticidade não possa ser demonstrada não oferece base confiável para decisões judiciais. A exigência de autenticidade relaciona-se ao princípio da mesmidade, a garantia de que o vestígio apresentado em juízo corresponda ao material efetivamente obtido durante a investigação (Prado, 2021a). Esse controle busca impedir que a seleção estatal do acervo probatório reduza o acesso da defesa ao conjunto integral de dados colhidos (Menezes; Borri; Soares, 2018).

A autenticidade também se relaciona ao princípio da desconfiança, segundo o qual nenhum elemento levado ao processo deve receber crédito prévio em razão de sua origem ou de quem o apresenta; a força probatória depende de mecanismos que permitam demonstrar a correspondência entre o objeto apresentado e aquilo que se afirma sobre ele, desde a obtenção até sua introdução em juízo (Menezes; Borri; Soares, 2018).

Os princípios da mesmidade e da desconfiança convergem para a noção de fiabilidade probatória desenvolvida por Prado (2021b). Nessa perspectiva, a cadeia de custódia constitui dimensão da “prova sobre a prova”, por fornecer elementos para a aferição da autenticidade e da integridade do vestígio digital.

Daí a indispensabilidade de procedimentos aptos a documentar a coleta, o manuseio, o transporte e a conservação de vestígios. Afinal, a violação da cadeia de custódia, por sua relação direta com garantias constitucionais, pode repercutir na admissibilidade, na valoração ou na licitude da prova, conforme a orientação doutrinária adotada.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Prado e Lopes Jr. sustentam que a violação compromete a licitude da prova, impondo sua inadmissibilidade ou exclusão do processo. Badaró, por sua vez, entende que a quebra repercute no plano da valoração probatória, sem afetar, por si só, a admissibilidade ou a validade do elemento probatório (Vieira; Santos, 2025).

Na posição defendida por Menezes, Borri e Soares (2018), a ruptura da cadeia de custódia pode retirar a confiabilidade do elemento probatório e conduzir ao reconhecimento de sua ilicitude. Quando outros elementos decorrerem diretamente da prova comprometida, o vício originário poderá também alcançar as provas derivadas, segundo a lógica da contaminação probatória.

Precedente do STJ ilustra a aplicação desses fundamentos. No RHC 218.358/PI, o extravio das gravações e imagens que serviram de base à elaboração de laudos periciais impediu o acesso às fontes originais. Embora não houvesse indícios de adulteração do material, a falha no armazenamento e conservação comprometeu a possibilidade de produção de contraprovas, rompendo, por conseguinte, a paridade de armas entre as partes. Reconheceu-se, por isso, a quebra da cadeia de custódia e a nulidade dos laudos periciais correspondentes (Brasil, 2025d).

Como os algoritmos *hash* atestam a integridade dos laudos, mas não suprem a ausência do material que os originou (Fisberg, 2025, p. 10), a nulidade declarada pelo STJ decorreu não de adulteração comprovada, mas da impossibilidade de a defesa exercer seus direitos processuais.

No mesmo sentido, o RHC 205.441/GO, também julgado pelo STJ, envolvia conversa extraída de telefone celular apreendido em diligência de busca e apreensão. Constatou-se que: (i) não havia menção a eventual lacre do aparelho nem registro do seu IMEI (*International Mobile Equipment Identity*); (ii) outro *smartphone* fora acautelado na mesma ocasião; (iii) o arquivo da conversa incriminadora encontrava-se em formato .txt, facilmente editável, tendo a perícia particular contratada pela defesa atestado sua modificação após a apreensão. O acórdão assentou ser dever do Estado a comprovação da integridade e da confiabilidade das provas, não sendo cabível simplesmente presumir a veracidade das alegações estatais quando descumpridos os procedimentos referentes à cadeia de custódia (Brasil, 2025c).

Em ambos os casos, a integridade e a confiabilidade das fontes de prova foram tratadas como ônus do Estado, com intensidade agravada nas provas digitais.

Como se verá adiante, a *blockchain* pode funcionar como estrutura para documentação e auditabilidade da cadeia de custódia, com potencial para mitigar sobretudo a segunda, a terceira e a quarta vulnerabilidades apontadas na seção 3.1 (acesso não registrado ao vestígio, falhas de lacre e acondicionamento e manipulação imperceptível de arquivos), além de atenuar

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

a quinta (disparidade entre acusação e defesa), por meio do acesso simétrico aos registros de custódia.

A primeira vulnerabilidade, de índole normativa, não se supera por via tecnológica, e mesmo o alcance das demais encontra limite em momentos anteriores ao registro. Afinal, como se examinará na seção 3.4, a *blockchain* não atesta a fidedignidade do que é gerado fora de seu ambiente (Problema do Oráculo), aspecto essencial para compreender por que ela não soluciona, por si, todas as vulnerabilidades inerentes à cadeia de custódia de vestígios forenses.

3.3. A tecnologia *blockchain*

A tecnologia *blockchain* surgiu de pesquisas em criptografia num contexto de desconfiança no sistema financeiro mundial. O desenvolvimento de algoritmos criptográficos sofisticados ocorria enquanto a crise financeira global de 2008 criava o ambiente para a emergência de mecanismos de transação que não dependessem de autoridade central para validação e garantia de confiabilidade. Foi nesse cenário que o indivíduo sob pseudônimo Satoshi Nakamoto apresentou, no artigo *Bitcoin: a peer-to-peer electronic cash system*, a proposta que daria origem à tecnologia *blockchain*, demonstrando como algoritmos criptográficos poderiam ser combinados com mecanismos de consenso descentralizado para criar um sistema monetário sem intermediários (Nakamoto, 2008).

Logo se percebeu que a inovação era transcendente ao escopo puramente monetário. Isto porque os mesmos princípios que permitiam rastrear a propriedade de bitcoins poderiam garantir a integridade de qualquer informação registrada na *blockchain*. A tecnologia evoluiu para uma infraestrutura de registro distribuído de propósito mais amplo. Conceitualmente, "*blockchain* é uma estrutura de dados que torna possível criar um livro-razão de dados digital e compartilhá-lo em uma rede de grupos independentes" (Laurence, 2018, p. 20).

Em termos computacionais, a *blockchain* consiste em uma estrutura de registro distribuído que organiza dados em blocos encadeados de forma cronológica, protegidos por mecanismos criptográficos que garantem sua integridade e rastreabilidade. O bloco é a unidade fundamental de armazenamento e organização de dados, uma estrutura composta pelo módulo de cabeçalho e pelo módulo lista de transações. Segundo Conceição e Rocha (2020, p. 34), "o cabeçalho consiste em diversos metadados que identificam unicamente o bloco. Já a lista de transações identifica as transações realizadas e contidas nesse bloco".

O cabeçalho funciona como uma espécie de "envelope identificador" porque, à semelhança de um documento de identidade, descreve a data de criação do bloco, seu posicionamento na sequência e suas características. Já a lista de transações contém o conteúdo

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

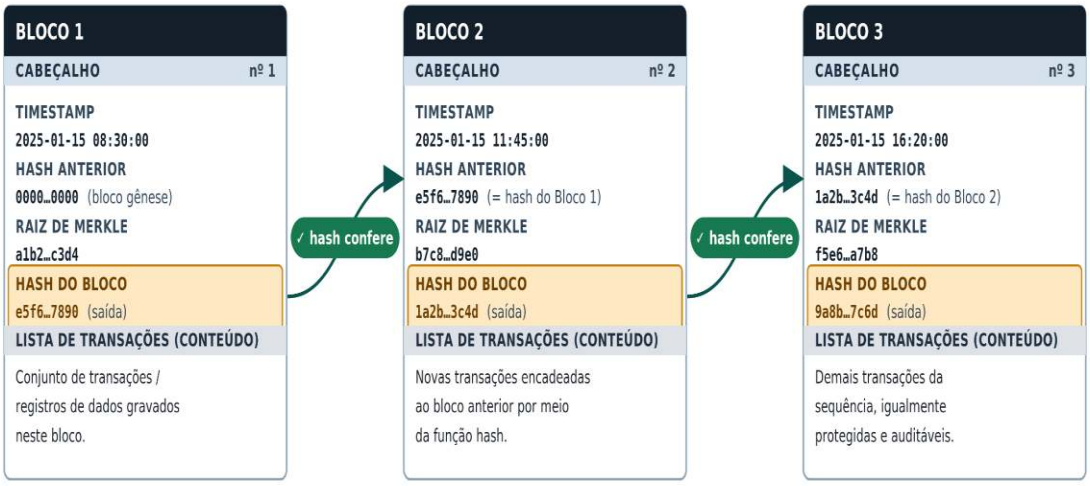
propriamente dito. Dois componentes do cabeçalho são centrais para os fins deste estudo: *timestamp* e *hash*.

O *timestamp* é uma marcação temporal criptográfica que difere da mera anotação de data e hora por estar permanentemente integrado à estrutura criptográfica do bloco, registrando o momento exato de sua criação e de cada manuseio, o que, para fins de cadeia de custódia, oferece comprovação de quando um vestígio foi fixado, recebido ou processado.

O *hash* estabelece a ligação criptográfica entre blocos consecutivos, criando a sequência encadeada que caracteriza a *blockchain*. Qualquer tentativa de alterar um bloco quebra a ligação com o seguinte, que por sua vez quebra a ligação com o próximo, em efeito cascata de invalidação que torna a fraude impossível de ocultar. Como ilustram Conceição e Rocha (2020, p. 16), "a *Blockchain* é como uma corrente. É fácil identificar se um elo da corrente foi rompido; o que significa que a corrente não está mais íntegra e não é mais confiável".

O cabeçalho contém, ainda, a raiz de Merkle, estrutura que resume todos os dados criptografados do bloco e funciona como verdadeira certidão de integridade. Isto porque a modificação de uma única informação altera a raiz, criando inconsistência detectável por qualquer validador da rede. A raiz de Merkle pode incluir o *nonce*, valor que integra o processo de criação e validação do bloco, conferindo a cada um exclusividade absoluta em sua estrutura de validação. A Figura 1 ilustra o encadeamento entre blocos e os campos do cabeçalho ora descritos.

Figura 1. Estrutura e encadeamento de blocos em uma rede *blockchain*



Fonte: os autores.

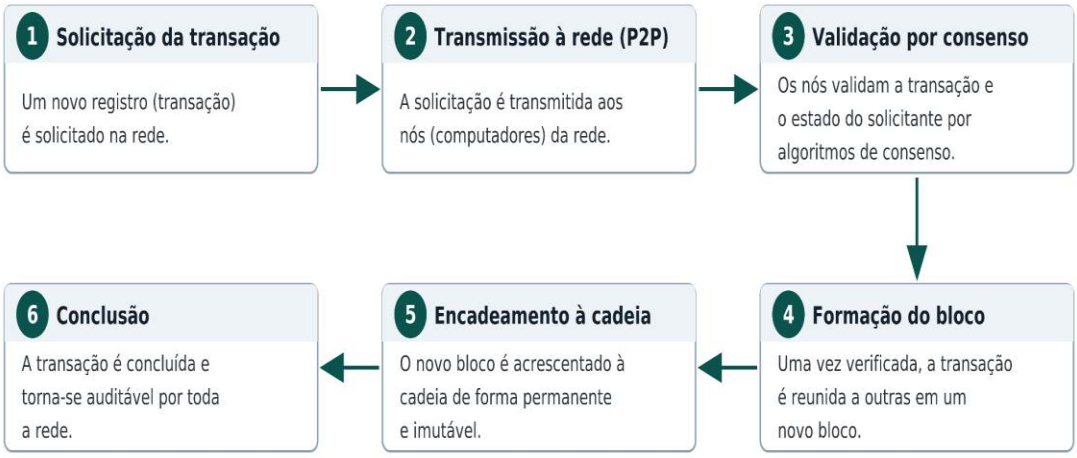
Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Como se percebe, cada bloco é composto por cabeçalho (*timestamp*, *hash* anterior, raiz de Merkle e *hash* do bloco) e pela lista de transações, que armazena o conteúdo registrado no bloco. O *hash* do bloco resume criptograficamente todo o seu conteúdo e é registrado como "*hash* anterior" do bloco seguinte, formando a corrente.

A integridade verifica-se pela coincidência entre o *hash* de um bloco e o "*hash* anterior" gravado no bloco posterior, representada na Figura 1 pelo selo "✓ *hash* confere". Enquanto essa correspondência se mantém em todos os elos, a sequência permanece íntegra e auditável.

Compreendida a estrutura interna do bloco, convém observar o seu funcionamento dinâmico, ou seja, o percurso de um registro desde a solicitação até a sua incorporação definitiva à cadeia. Esse ciclo esclarece por que a tecnologia dispensa uma autoridade central de validação: cada nova transação é transmitida a uma rede de nós (computadores) que a validam coletivamente, por mecanismos de consenso, antes de reuni-la a outras em um novo bloco encadeando-a de forma permanente aos blocos anteriores. A Figura 2 sintetiza esse ciclo de vida de uma transação na rede.

Figura 2. Ciclo de vida de uma transação em uma rede *blockchain*



Fonte: adaptado de Lamounier (2018), publicado em 101 *Blockchain*s.

É justamente essa validação distribuída que confere à *blockchain* a sua principal característica: a ausência de um ponto único de controle e, por consequência, de falha ou de manipulação.

Esses elementos respondem a dilemas práticos enfrentados na preservação de vestígios criminais. A imutabilidade do registro em *blockchain* pode garantir que um vestígio não foi

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

alterado ou removido sem que tal manipulação seja detectável. Resta examinar como essa infraestrutura pode ser aplicada à cadeia de custódia de vestígios no processo penal brasileiro.

3.4. *Blockchain* na cadeia de custódia de vestígios

As propriedades anteriormente descritas incidem sobre vulnerabilidades próprias das etapas de fixação, recebimento e processamento previstas no art. 158-B do CPP (Brasil, 2019). Como observa Pastore (2020, p. 77), a mutabilidade dos dados digitais pode comprometer a confiabilidade da prova quando não são adotados procedimentos técnicos adequados. Essa mesma infraestrutura, contudo, pode ampliar a verificabilidade da origem e da preservação do conteúdo, desde que a coleta, o armazenamento, a extração e o registro dos dados sejam conduzidos com mecanismos capazes de demonstrar sua autenticidade e integridade.

A *blockchain* é precisamente o mecanismo tecnológico de cautela que transforma a fragilidade do suporte digital em uma solução adequada no que diz respeito à cadeia de custódia de vestígios criminais. Isto porque, ao se registrar o *hash* de cada evento, seja de fixação, de recebimento ou de processamento de provas, o registro abrange a garantia de *timestamp* criptográfico e é imutável.

Transpondo a lógica geral exposta na seção anterior para o domínio probatório, cada uma das três etapas críticas do art. 158-B passa a constituir um bloco da cadeia: a fixação registra o estado original do vestígio; o recebimento documenta a transferência de posse; e o processamento, o exame pericial. O *hash* de cada etapa é gravado como "*hash* anterior" da seguinte, de modo que a sequência custodial inteira se torna encadeada e auditável, conforme ilustra a Figura 3.

Figura 3. Aplicação do encadeamento de blocos às etapas de fixação, recebimento e processamento da cadeia de custódia



Fonte: os autores.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Cada bloco preserva, em seu cabeçalho, o *timestamp* criptográfico e o *hash* que o vincula ao anterior; na lista de transações, registra o conteúdo do respectivo ato custodial. O exame de cada uma dessas etapas, a seguir, evidencia a vulnerabilidade específica e a resposta que a *blockchain* oferece.

Na etapa de fixação (Brasil, 2019, art. 158-B, inc. III), enquanto no mundo físico a materialidade do meio permite, por exemplo, exames grafotécnicos e análise de tinta e papel para verificar autenticidade, a modificação de registros eletrônicos pode dificultar, ou até impedir, a identificação posterior de alterações, conforme as características do suporte e os procedimentos de preservação empregados (Pastore, 2020, p. 67-68).

A *blockchain* pode contribuir mediante o registro do identificador criptográfico (*hash*) atribuído a cada arquivo no momento de sua fixação, associado a uma marca temporal (*timestamp*). O *hash* funciona como uma representação derivada do conteúdo: qualquer mudança tende a produzir resultado diverso quando o arquivo é novamente submetido ao mesmo algoritmo. A divergência entre os códigos, portanto, indica que o conteúdo examinado não corresponde ao arquivo originalmente registrado; sua coincidência, por sua vez, constitui elemento técnico relevante para a verificação de integridade (Pastore, 2020, p. 69-70).

O fluxo composto pela captura do arquivo no local do crime, pela geração imediata de seu identificador criptográfico (*hash*) e pelo registro documentado das pessoas responsáveis por sua manipulação contribui para a demonstração da autenticidade e da integridade do vestígio digital. Essa documentação é relevante para que o exame da confiabilidade do elemento probatório anteceda sua valoração, pois a cadeia de custódia deve permitir verificar quem teve contato com a prova e quais mecanismos foram empregados para preservar seu conteúdo (Vieira; Santos, 2025).

O registro desse fluxo em *blockchain*, associado a marca temporal (*timestamp*), constitui aplicação tecnológica proposta neste estudo para reforçar a rastreabilidade e a verificabilidade dos eventos de custódia. O uso do *hash*, contudo, deve ser compreendido como um mecanismo de aferição de integridade do arquivo ou pacote de dados, não como garantia autônoma da autenticidade da fonte ou da validade integral da prova (Fisberg, 2025).

Ainda que desprovida de força de lei e, portanto, incapaz de suprir a lacuna legislativa apontada na seção 3.1, a ABNT NBR ISO/IEC 27037 oferece parâmetro técnico de referência para o tratamento da evidência digital. A norma orienta o seu manuseio segundo critérios de auditabilidade, justificabilidade, repetibilidade e reprodutibilidade, mediante procedimento estruturado em identificação, coleta, aquisição e preservação (ABNT, 2013; Vieira; Santos,

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

2025). Tais diretrizes podem ser empregadas, de modo complementar, para concretizar as etapas previstas no art. 158-B do CPP.

São essas diretrizes que a *blockchain* operacionaliza de modo automático e sistemático, ao registrar o *hash* de cada evento custodial em cadeia imutável e auditável, indicando o caminho normativo que se espera ver futuramente positivado.

No mesmo sentido, e já com força normativa porque incorporada ao direito brasileiro (Brasil, 2023a), a Convenção de Budapeste exige, em seu art. 16, a preservação da integridade dos dados digitais.

Na etapa de recebimento (Brasil, 2019, art. 158-B, inc. VII), a continuidade documental da custódia é indispensável para demonstrar que o vestígio encaminhado à análise corresponde ao material originalmente recolhido. A insuficiência dos registros sobre a transferência de posse pode fragilizar a demonstração da custódia e a aferição da identidade e integridade do vestígio (Brandão, 2021).

Pastore (2020) ressalta que a confiabilidade do material exige controle sobre quem o manipula e documentação das condições de sua guarda e deslocamento. Para esse fim, mostram-se relevantes os registros relativos à entrega e ao recebimento, à identificação dos responsáveis, ao uso de lacres, ao transporte e ao acondicionamento, de modo a permitir a reconstituição do percurso do vestígio e a verificação de sua autenticidade e integridade. Essa exigência evidencia a falha examinada no HC 653.515/RJ, analisada na seção 3.1.

No caso da *blockchain*, o registro de cada transferência de posse gera um novo bloco na cadeia, contendo *timestamp* criptográfico específico, identificação das partes, código do lacre e *hash*; o efeito cascata de invalidação garante que qualquer adulteração na sequência de custódias seja detectável.

A *blockchain* também pode contribuir para reduzir a assimetria entre acusação e defesa, ao oferecer à defesa meios independentes para analisar a integridade de evidências digitais. Nessa perspectiva, a tecnologia amplia as condições de paridade entre as partes, sem depender exclusivamente da iniciativa ou da diligência dos órgãos estatais de persecução (Vilela; Assis; Eduardo, 2025).

Na etapa de processamento (Brasil, 2019, art. 158-B, inc. VIII), a vulnerabilidade no caso de arquivos digitais sem o uso da *blockchain* é duplamente identificada. Isto porque, em termos operacionais, qualquer acesso ao suporte digital sem registro da operação permite inserção, exclusão ou alteração indetectável de arquivos (situação reconhecida no AgRg no RHC 143.169/RJ, referido na seção 3.1).

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

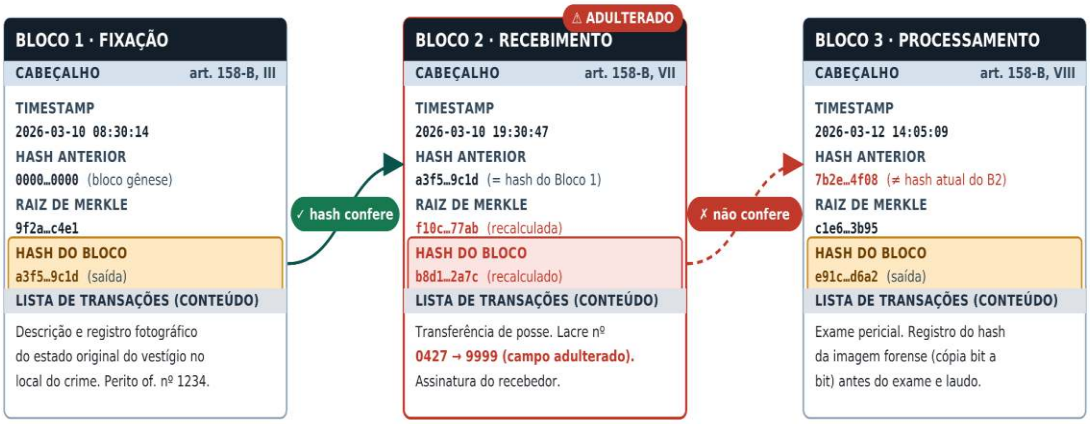
Processualmente, a ausência de duplicação forense desloca a análise para a própria fonte original da prova digital, em vez de permitir que ela recaia sobre uma cópia integral verificada e validada por *hash*. Isso compromete tanto a preservação do vestígio originário, quanto a possibilidade de controle posterior pela defesa, inclusive para fins de contraprova.

A resposta da *blockchain* não está na substituição da duplicação forense, mas no registro do *hash* da imagem forense (cópia integral dos arquivos originais) antes do início do exame pericial. Forma-se, assim, uma referência verificável de integridade, já que a divergência entre o *hash* originalmente registrado e aquele obtido da cópia indica que o conteúdo não permaneceu idêntico.

Além disso, a consulta a esse registro pela defesa pode viabilizar a comparação entre a cópia disponibilizada para o controle defensivo e aquela efetivamente examinada pela acusação. Como exemplo de preservação de conteúdo digital em *blockchain*, Vilela, Assis e Eduardo (2025) relatam a utilização da plataforma OriginalMy para registrar publicações ofensivas em redes sociais, permitindo sua remoção posterior sem inviabilizar seu aproveitamento no processo penal. A solução preservava informações sobre a existência do conteúdo, a data e a hora do registro (*timestamp*) e possíveis alterações posteriores.

O encadeamento descrito nas três etapas converte a adulteração em evento detectável. Caso qualquer registro custodial seja alterado (como, por exemplo, a substituição do conteúdo no recebimento), o *hash* daquele bloco é recalculado e deixa de corresponder ao "*hash* anterior" já gravado no bloco seguinte, rompendo o elo e invalidando, em cascata, todos os registros posteriores. A Figura 4 representa essa ruptura.

Figura 4. Detecção da ruptura da cadeia de custódia diante da adulteração de um registro



Fonte: os autores.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Diferentemente do que ocorre nos sistemas documentais tradicionais, em que a alteração retroativa pode passar despercebida (como evidenciado nos precedentes examinados na seção 3.2), na cadeia em *blockchain* a adulteração não pode ser ocultada porque ela se manifesta na própria estrutura criptográfica do registro.

A demonstração da aptidão tecnológica, contudo, não é suficiente, pois sua implementação depende de respaldo normativo. No plano internacional, o *Financial Innovation and Technology for the 21st Century Act* (FIT21), aprovado nos Estados Unidos da América, o *Markets in Crypto-Assets Regulation* (MiCA) da União Europeia, e a *Virtual Assets Regulatory Authority* (VARA) dos Emirados Árabes Unidos, indicam convergência quanto à necessidade de padrões técnicos obrigatórios de preservação, auditoria e rastreabilidade de informações em ambientes digitais (Estados Unidos, 2024; União Europeia, 2023; Emirados Árabes Unidos, 2022).

O FIT21 exige documentação cronológica das transações com assinaturas digitais, protocolos de verificação independente e carimbos de tempo (Estados Unidos, 2024). O MiCA impõe segregação de ativos, registro transparente de transações e auditorias periódicas independentes, requisitos que espelham, em essência, o conceito jurídico de cadeia de custódia probatória (União Europeia, 2023). A VARA centraliza a supervisão de ativos virtuais em autoridade independente, com manutenção de registros auditáveis e detalhados de todas as operações (Emirados Árabes Unidos, 2022).

Embora concebidas para mercados financeiros, essas normativas estabelecem parâmetros que transcendem a esfera econômica e reforçam o argumento da necessidade de complementar o art. 158-B do CPP com diretrizes específicas sobre custódia digital, preferencialmente alinhadas aos padrões internacionais.

No Brasil, em âmbito legislativo, o Projeto de Lei (PL) 4.939/2020 fixa critérios para a obtenção e a admissibilidade de provas digitais. Regulamenta procedimentos específicos de preservação digital (art. 13) e estipula, no art. 19, a autenticidade, a integridade, a completude, a auditabilidade e a reprodutibilidade como princípios norteadores (Brasil, 2020). O PL 1.195/2025, por sua vez, visa alterar a Medida Provisória 2.200-2/2001 para incluir a *blockchain* como meio de comprovação de transações, definindo-a como registro digital em livro-razão compartilhado e imutável, com status de assinatura eletrônica avançada (Brasil, 2025a).

No Poder Judiciário, a Portaria 391/2025, da Presidência do CNJ, instituiu Grupo de Trabalho (GT) com escopo de elaborar propostas normativas para a disciplina e a preservação da cadeia de custódia de provas digitais. O GT também tem atribuições para propor

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

especificações técnicas de armazenamento e rastreabilidade de vestígios e para estruturar ferramentas tecnológicas que podem ser baseadas em *blockchain* (Brasil, 2025b).

O Poder Executivo federal mantém iniciativas que evidenciam a viabilidade operacional da *blockchain* em serviços públicos. A emissão da Carteira de Identidade Nacional (CIN) utiliza o Cadastro Compartilhado da Receita Federal (b-Cadastros) para viabilizar, entre a Receita Federal do Brasil (RFB) e Órgãos de Identificação Civil (OICs), operações de consulta, inscrição e alteração no Cadastro de Pessoa Física (CPF) e na própria CIN (Brasil, 2023b).

A mesma infraestrutura constitui uma plataforma de compartilhamento de bases cadastrais estruturada como rede *blockchain* permissionada: Cadastro de Pessoa Física (CPF), Cadastro Nacional da Pessoa Jurídica (CNPJ), Cadastro Nacional de Obras (CNO), Cadastro de Atividade Econômica da Pessoa Física (CAEPF), Simples Nacional e Dívida Ativa da União (SERPRO, 2023).

Não obstante esses avanços, relevantes desafios ainda condicionam a implementação da *blockchain* na cadeia de custódia de provas digitais. O desafio técnico consiste em tratá-la como solução autossuficiente para todas as etapas do ciclo probatório. A tecnologia pode reforçar a integridade, a rastreabilidade e a auditabilidade de registros já produzidos, mas não substitui as fases anteriores de isolamento, de coleta, de captura e de duplicação forense do vestígio. Afinal, se dados falsos, incompletos ou adulterados forem registrados, a *blockchain* apenas preservará, de modo imutável, uma informação originariamente inadequada.

Trata-se do denominado Problema do Oráculo, que se refere à dificuldade de introduzir em uma *blockchain* informações sobre eventos ou estados ocorridos fora da rede sem reintroduzir vínculos de confiança com as fontes, os agentes de coleta ou os mecanismos de transmissão desses dados. No contexto da cadeia de custódia, o problema manifesta-se quando a informação registrada, como o *hash* de um arquivo, a data de apreensão, a identidade do responsável pela coleta ou o evento de transferência de posse, depende de um ato humano, de um dispositivo ou de uma base externa anterior ao registro em *blockchain*. A imutabilidade da rede preserva a integridade do dado inserido a partir daquele momento, mas não certifica, por si só, a correspondência entre o registro e o evento físico ou digital que ele pretende representar (Egberts, 2017; Al-Breiki et al., 2020; Pasdar; Lee; Dong, 2023).

Assim, se um agente mal-intencionado ou tecnicamente despreparado registrar *hashes* de arquivos adulterados, metadados incorretos ou eventos de custódia inexistentes, a *blockchain* não corrigirá o defeito antecedente: apenas preservará de modo verificável o registro produzido a partir daquele instante.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

Essa limitação mostra que a adoção da *blockchain* somente é compatível com o processo penal quando integrada a protocolos objetivos de coleta, de documentação, de validação e de controle, convergentes com a advertência de Lopes Jr. e Morais da Rosa (2015), para quem “a discussão acerca da subjetividade deve dar lugar a critérios objetivos, empiricamente comprováveis, que independam da prova de má-fé ou ‘bondade e lisura’ do agente estatal”.

Para mitigar o Problema do Oráculo na atividade policial de campo, é necessário reduzir os espaços de discricionariedade humana no registro inicial do vestígio e tornar auditáveis as etapas anteriores ao ingresso do dado na rede. Isso envolve, por exemplo, vincular a geração do *hash* à captura do arquivo, registrar automaticamente a identidade do dispositivo e do agente responsável, documentar a origem dos metadados e permitir verificação independente dos registros. Isto porque a descentralização, a multiplicidade de fontes e os mecanismos de validação inerentes à *blockchain* não dispensam controles sobre a qualidade e a independência das fontes utilizadas (Egberts, 2017; Al-Breiki et al., 2020; Pasdar; Lee; Dong, 2023).

Nessa perspectiva, destaca-se o GT-ChainGuard, iniciativa desenvolvida no âmbito do Projeto Ilíada na Universidade Federal do Pará (UFPA). O projeto propõe o emprego da *blockchain* para assegurar a integridade, a autenticidade e a rastreabilidade da cadeia de custódia de evidências digitais (Observatório Nacional de *Blockchain*, 2025).

A solução compreende uma aplicação *web* voltada à gestão e à auditoria da cadeia de custódia e um aplicativo móvel destinado à coleta de vestígios em campo, inclusive em locais sem conectividade. No momento da captura de imagens, o aplicativo opera em modo *offline*, gera automaticamente o *hash* do arquivo e registra metadados criptográficos, tais como geolocalização, data, hora e informações do dispositivo. Uma vez restabelecida a conexão, tais registros são sincronizados e preservados em rede *blockchain*, permitindo o registro imutável das ações relacionadas às evidências (Observatório Nacional de *Blockchain*, 2025).

No plano jurídico, o desafio envolve incompatibilidade entre as propriedades intrínsecas da *blockchain* e as diretrizes da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), que assegura aos titulares direitos de retificação e exclusão definitiva de registros; direitos inconciliáveis com redes concebidas sob a premissa de que nenhum dado inserido pode ser excluído ou alterado.

No inquérito policial, por exemplo, o espelhamento de celulares apreendidos pode resultar em coleta de dados de terceiros estranhos à investigação, cuja perenização na *blockchain* configura violação à LGPD. A compatibilização demanda o desenvolvimento de redes híbridas, nas quais o conteúdo sensível permanece em bases de dados mutáveis convencionais

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

(*off-chain*), sujeitas à exclusão ordenada pelo juiz, enquanto apenas dados de auditoria e *hashes* de integridade são gravados de forma perene no livro distribuído (*on-chain*) (Stevan; Cruz, no prelo).

Essa arquitetura, ao reservar à camada *on-chain* apenas metadados de integridade enquanto os dados pessoais permanecem em repositório *off-chain* removível, viabiliza a exclusão de dados relativos à LGPD (Stevan; Cruz, no prelo), sem comprometer a cadeia criptográfica de custódia do vestígio investigativo.

Sob a perspectiva institucional, o desafio é a falta de parâmetros uniformes para o trato da cadeia de custódia de evidências criminais. A superação dessa lacuna passa por dois vetores normativos complementares, já identificados ao longo desta seção.

No plano legislativo situam-se os instrumentos de maior alcance. Por terem o potencial para gerar normas com status de lei federal, o PL 4.939/2020, que disciplina a preservação e a admissibilidade da prova digital e fixa, no art. 19, os princípios da autenticidade, integridade, auditabilidade e reprodutibilidade, e o PL 1.195/2025, que reconhece a *blockchain* como meio idôneo de comprovação, teriam eficácia vinculante sobre todos os órgãos de persecução penal (inclusive na fase investigativa, em que se concentra a maior parte dos atos de coleta e preservação do vestígio). É justamente nessa fase, alheia à atuação direta do Judiciário, que a padronização normativa se mostra mais urgente.

No plano regulamentar, a futura resolução do CNJ, resultante do GT instituído pela Portaria 391/2025 para disciplinar a preservação da cadeia de custódia da prova digital, constitui vetor relevante de padronização. Ainda que seu alcance se restrinja ao Poder Judiciário, suas resoluções têm potencial para influenciar a forma como as evidências ingressam no processo judicial, podendo, ademais, antecipar e detalhar tecnicamente parâmetros que a legislação venha a consagrar.

Em suma, os resultados demonstram que a *blockchain* constitui mecanismo potencialmente relevante (porém não suficiente) para assegurar a autenticidade e a integridade probatórias no processo penal brasileiro. Pode reforçar, a partir do momento do registro, as condições de verificação associadas aos princípios da mesmidade e da desconfiança, mas não alcança as falhas de autenticidade anteriores à inserção dos dados (Problema do Oráculo, examinado acima), nem dispensa arquitetura híbrida compatível com a proteção de dados pessoais e regulamentação que unifique os procedimentos em âmbito nacional.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

4. CONSIDERAÇÕES FINAIS

Este artigo partiu da hipótese de que a implementação da tecnologia *blockchain* nas etapas de fixação, recebimento e processamento da cadeia de custódia, previstas no art. 158-B do CPP, seria suficiente para garantir a autenticidade e a integridade probatórias diante do risco de adulteração de evidências, proporcionando segurança jurídica superior à dos métodos convencionais de documentação.

A análise confirmou que os arts. 158-A a 158-F do CPP estabeleceram as etapas da cadeia de custódia sem disciplinar seus protocolos técnicos. Essa lacuna ficou evidente em decisões do STJ (HC 653.515/RJ e AgRg no RHC 143.169/RJ), que expuseram a fragilidade de registros documentais suscetíveis de adulteração retroativa, bem como a falta de uma trilha de auditoria objetiva.

O debate sobre as consequências processuais da quebra da cadeia de custódia, os princípios da mesmidade e da desconfiança, a contaminação das provas derivadas do vestígio maculado e, segundo precedentes do STJ (RHC 218.358 e RHC 205.441), indicam que o processo penal, no que diz respeito à cadeia de custódia, permanece atualmente exposto a condenações fundadas em provas adulteradas e a absolvições decorrentes de falhas evitáveis na custódia dos vestígios.

Elementos inerentes à *blockchain*, como o encadeamento criptográfico de blocos, o *timestamp*, a função *hash* e a raiz de Merkle respondem a essas fragilidades. Afinal, a imutabilidade torna detectável qualquer adulteração retroativa, o *timestamp* assegura precisão cronológica e a descentralização elimina o ponto único de falha dos sistemas tradicionais de registro. Aplicados às três etapas selecionadas, esses atributos evidenciaram, em cada uma, a vulnerabilidade específica e a resposta técnica correspondente.

Os panoramas normativos internacional e doméstico apontam para regulamentações em torno da auditoria de registros digitais. No âmbito comparado, destacam-se o FIT21, o MiCA e a VARA; no cenário brasileiro, o possível avanço normativo encontra-se nos PLs 4.939/2020 e 1.195/2025, bem como na Portaria CNJ 391/2025.

Restam, contudo, condicionantes que delimitam o alcance da tecnologia. Sua capacidade de reforçar a autenticidade probatória depende da correção e da confiabilidade dos dados no momento de sua inserção na rede (Problema do Oráculo), pois a *blockchain* assegura a integridade do registro, mas não comprova a veracidade do evento externo, a legitimidade da fonte nem a correção dos procedimentos que antecedem o registro na rede.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

A isso se soma a tensão entre a imutabilidade da rede e os direitos de retificação e exclusão assegurados pela LGPD, a impor a adoção de arquiteturas híbridas, com preservação *off-chain* do conteúdo e registro *on-chain* apenas de identificadores criptográficos e marcas temporais.

No plano probatório, a *blockchain* pode ser compreendida como mecanismo complementar de controle epistêmico; ao registrar elementos verificáveis sobre a origem e a preservação dos dados, contribui para o exame de fiabilidade da própria prova.

Assim, a hipótese confirma-se apenas em parte. A *blockchain* mostra-se tecnicamente adequada para endereçar as vulnerabilidades das etapas de fixação, recebimento e processamento da cadeia de custódia, previstas no art. 158-B do CPP, assegurando a integridade dos registros a partir de sua inserção na rede, e oferece segurança jurídica superior à dos métodos convencionais de documentação, mas não é suficiente de forma autônoma.

Reconhecem-se as limitações do estudo, de abordagem teórico-dogmática e sem validação empírica em órgãos periciais brasileiros, ao que se soma a tramitação ainda inconclusa do marco normativo nacional.

Daí decorre uma agenda de pesquisa voltada às condicionantes identificadas: o enfrentamento do Problema do Oráculo, a compatibilização entre a imutabilidade da rede e a proteção de dados pessoais, por meio de arquiteturas híbridas e a elaboração de regulamentação uniforme em âmbito nacional.

REFERÊNCIAS

AL-BREIKI, Hamda; REHMAN, Muhammad Habib Ur; SALAH, Khaled; SVETINOVIC, Davor. Trustworthy *blockchain* oracles: review, comparison, and open research challenges. **IEEE Access**, v. 8, p. 85675-85685, 2020. Disponível em: https://doi.org/10.1109/ACCESS.2020.2992698. Acesso em: 5 jul. 2026.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27037:2013**: Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

BECCARIA, Cesare. **Dos delitos e das penas**. São Paulo: Martins Fontes, 2015.

BRANDÃO, Bruno Monteiro de Castro. **A quebra da cadeia de custódia e suas consequências**. In: CAMBI, Eduardo; SILVA, Danni Sales; MARINELA, Fernanda (org.). Pacote anticrime: volume II. Curitiba: Escola Superior do MPPR, 2021. p. 107-121. Disponível em: https://www.cnmp.mp.br/portal/images/Publicacoes/documentos/2021/Pacote_Anticrime_volume_2.pdf. Acesso em: 4 jun. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

BRASIL. Câmara dos Deputados. **Projeto de Lei n. 1.195, de 2025. Altera a Medida Provisória n. 2.200-2, de 24 de agosto de 2001, para normatizar o uso da ferramenta *blockchain***. Brasília, DF: Câmara dos Deputados, 2025a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2488682. Acesso em: 27 maio 2026.

BRASIL. Câmara dos Deputados. **Projeto de Lei n. 4.939, de 2020**. Estabelece as diretrizes do direito da Tecnologia da Informação. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1966324. Acesso em: 25 maio 2026.

BRASIL. Conselho Nacional de Justiça. **Portaria n. 391, de 4 de novembro de 2025. Institui Grupo de Trabalho para a elaboração de estudos e propostas pertinentes à disciplina e à preservação da cadeia de custódia da prova digital**. Diário da Justiça Eletrônico do CNJ, Brasília, DF, n. 248, p. 15-16, 7 nov. 2025b. Disponível em: https://atos.cnj.jus.br/atos/detalhar/6418. Acesso em: 25 maio 2026.

BRASIL. Conselho Nacional de Justiça. **Justiça em números 2026**. Brasília, DF: CNJ, 2026. Disponível em: https://www.cnj.jus.br/pesquisas-judiciarias/justica-em-numeros/. Acesso em: 7 jul. 2026.

BRASIL. **Decreto n. 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Cibercrime, firmada em Budapeste, em 23 de novembro de 2001**. Diário Oficial da União, Brasília, DF, 13 abr. 2023a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 2 abr. 2026.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03.old/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 jun. 2026.

BRASIL. Lei n. **13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal**. Diário Oficial da União: seção 1, Brasília, DF, 24 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03.old/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 21 jun. 2026.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Governo começa a utilizar o *blockchain* na emissão da Carteira de Identidade Nacional**. Brasília, DF, 26 set. 2023b. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/setembro/governo-comeca-a-utilizar-o-*blockchain*-na-emissao-da-carteira-de-identidade-nacional. Acesso em: 22 jun. 2026.

BRASIL. Ministério da Justiça. Secretaria Nacional de Segurança Pública. **Portaria n. 82, de 16 de julho de 2014. Estabelece as diretrizes sobre os procedimentos a serem observados no tocante à cadeia de custódia de vestígios**. Diário Oficial da União: seção 1, Brasília, DF, n. 136, p. 42, 18 jul. 2014.

BRASIL. Superior Tribunal de Justiça. **AgRg no RHC n. 143.169/RJ**. Relator: Ministro Messod Azulay Neto. Relator para acórdão: Ministro Ribeiro Dantas. Quinta Turma, julgado em 7 fev. 2023. Diário da Justiça Eletrônico, Brasília, DF, 2 mar. 2023c.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

BRASIL. Superior Tribunal de Justiça. **HC n. 653.515/RJ**. Relator: Ministro Rogerio Schietti Cruz. Sexta Turma, julgado em 23 nov. 2021. Diário da Justiça Eletrônico, Brasília, DF, 1 fev. 2022.

BRASIL. Superior Tribunal de Justiça. **RHC n. 205.441/GO**. Relator: Ministro Rogerio Schietti Cruz. Sexta Turma, julgado em 9 mai. 2025. Diário da Justiça Eletrônico Nacional, Brasília, DF, 14 maio 2025c.

BRASIL. Superior Tribunal de Justiça. **RHC n. 218.358/PI**. Relator: Ministro Sebastião Reis Júnior. Sexta Turma, julgado em 4 nov. 2025. Diário da Justiça Eletrônico Nacional, Brasília, DF, 11 nov. 2025d.

CHINA. Cyberspace Administration of China. ***Blockchain* Information Service Management Regulations**. Order n. 3, 10 jan. 2019. Beijing, 2019. Disponível em: https://www.cac.gov.cn/2019-01/10/c_1123971164.htm. Acesso em: 25 ago. 2025.

CONCEIÇÃO, Arlindo F. da; ROCHA, Vladimir E. M. ***Blockchain***: conceitos básicos e aplicações. Porto Alegre: Sociedade Brasileira de Computação, 2020.

EGBERTS, Alexander. **The Oracle Problem**: an analysis of how *blockchain* oracles undermine the advantages of decentralized ledger systems. 2017. Master's thesis (Business Sciences) — EBS Business School, Wiesbaden, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3382343. Acesso em: 22 jun. 2026.

EMIRADOS ÁRABES UNIDOS. Dubai Virtual Assets Regulatory Authority. **Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai**. Dubai, 2022. Disponível em: https://rulebooks.vara.ae/rulebook/law-no-4-2022-regulating-virtual-assets-emirate-dubai. Acesso em: 27 ago. 2025.

ESTADOS UNIDOS. Congress. House of Representatives. **H.R. 4763: Financial Innovation and Technology for the 21st Century Act**. 118th Congress, 2nd Session. Washington, DC, 2024. Disponível em: https://www.congress.gov/bill/118th-congress/house-bill/4763. Acesso em: 27 ago. 2025.

FISBERG, Yuri. Função 'hash' e a integridade da prova digital. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 11, n. 3, e1227, set./dez. 2025. Disponível em: https://doi.org/10.22197/rbdpp.v11i3.1227. Acesso em: 4 jul. 2026.

LAMOUNIER, Lucas. **Tecnologia *blockchain***: o guia definitivo para iniciantes. 101 *Blockchain*s, 12 set. 2018. Disponível em: https://101*blockchain*s.com/pt/tecnologia-*blockchain*-guia/. Acesso em: 23 mai. 2026.

LAURENCE, Tiana. ***Blockchain* para leigos**. Rio de Janeiro: Alta Books, 2018.

LOPES JÚNIOR, Aury; MORAIS DA ROSA, Alexandre. **A importância da cadeia de custódia para preservar a prova penal**. Consultor Jurídico, São Paulo, 16 jan. 2015. Disponível em: https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal/. Acesso em: 2 fev. 2026.

MENEZES, Isabela Aparecida de; BORRI, Luiz Antonio; SOARES, Rafael Junior. A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro. Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 4, n. 1, p. 277-300, jan./abr. 2018. DOI:

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

10.22197/rbdpp.v4i1.128. Disponível em: https://doi.org/10.22197/rbdpp.v4i1.128. Acesso em: 23 maio 2026.

NAKAMOTO, Satoshi. **Bitcoin**: a peer-to-peer electronic cash system. [S. l.: s. n.], 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 5 maio 2026.

OBSERVATÓRIO NACIONAL DE *BLOCKCHAIN*. **GT-ChainGuard**: cadeia de custódia de evidências digitais. Apresentação no 7º Encontro da Comunidade de Especialistas em *Blockchain*, 18 nov. 2025. Disponível em: https://observatorio*blockchain*.org.br/wp-content/uploads/2025/11/gt_chainguard.pdf. Acesso em: 4 jul. 2026.

PASDAR, Amirmohammad; LEE, Young Choon; DONG, Zhongli. **Connect API with *blockchain***: a survey on *blockchain* oracle implementation. ACM Computing Surveys, New York, v. 55, n. 10, art. 208, 2023. DOI: 10.1145/3567582. Disponível em: https://doi.org/10.1145/3567582. Acesso em: 5 jul. 2026.

PASTORE, Guilherme de Siqueira. **Considerações sobre a autenticidade e a integridade da prova digital**. Cadernos Jurídicos, São Paulo, ano 21, n. 53, p. 63-79, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/i_5_considera%C3%A7%C3%B5es_autenticidade.pdf?d=637250343071305756. Acesso em: 5 jul. 2026.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. 2. ed. São Paulo: Marcial Pons, 2021a.

PRADO, Geraldo. **Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital**. Texto correspondente à palestra "A interface entre o Direito Digital e o Processo Penal", proferida no Ciclo Permanente de Palestras do Núcleo de Estudo Luso-Brasileiro da Faculdade de Direito da Universidade de Lisboa, em 20 jan. 2021. Geraldo Prado, 22 jan. 2021b. Disponível em: https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/. Acesso em: 10 jun. 2026.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO). **Cadastro Compartilhado da Receita Federal**. Brasília, DF, 29 dez. 2023. Disponível em: https://bcadastros.serpro.gov.br/documentacao/. Acesso em: 22 jun. 2026.

STEVAN, Aléxia Liz Narok; CRUZ, Fabrício Bittencourt da. *Blockchain*, LGPD e o direito ao esquecimento: guia interativo de letramento jurídico-tecnológico como dispositivo de justiça cognitiva. **Humanidades & Inovação**, no prelo.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. **Regulamento (UE) n. 910/2014, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE**. Jornal Oficial da União Europeia, L 257, p. 73-114, 28 ago. 2014. Disponível em: https://eur-lex.europa.eu/eli/reg/2014/910/oj?locale=pt. Acesso em: 5 jul. 2026.

UNIÃO EUROPEIA. Parlamento Europeu; Conselho. **Regulamento (UE) 2023/1114, de 31 de maio de 2023, relativo aos mercados de criptoativos e que altera os Regulamentos (UE) n. 1093/2010 e (UE) n. 1095/2010 e as Diretivas 2013/36/UE e (UE) 2019/1937**. Jornal Oficial da União Europeia, 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32023R1114. Acesso em: 6 jun. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.

VIEIRA, Andrey Bruno Cavalcante; SANTOS, Hugo Leonardo Rodrigues. Investigação criminal e tecnologias digitais: algumas reflexões sobre o policiamento preditivo e a admissibilidade de provas digitais. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 11, n. 1, e1072, jan./abr. 2025. Disponível em: https://doi.org/10.22197/rbdpp.v11i1.1072. Acesso em: 3 mar. 2026.

VILELA, Matheus Dantas; ASSIS, Daniel Araújo de; EDUARDO, Pablo. ***Blockchain* e processo penal**: os reflexos dos avanços tecnológicos na confiabilidade da prova penal. VirtuaJus, Belo Horizonte, v. 10, n. 18, p. 295-308, 2025. Disponível em: https://doi.org/10.5752/P.1678-3425.2025v10n18p295-308. Acesso em: 10 mar. 2026.

Este artigo é publicado em acesso aberto (Open Access) sob a licença Creative Commons Atribuição 4.0 Internacional (CC-BY), que permite uso, distribuição e reprodução irrestritos em qualquer meio, desde que o autor original e a fonte sejam creditados.